Kingston IronKey D500S hardware-encrypted USB flash drive

FIPS 140-3 Level 3 (pending) certified, XTS-AES 256-bit hardware encrypted, rugged zinc casing

The best-in-class Kingston IronKey™ D500S/SM USB flash drive features flagship military-grade security that makes IronKey the most trusted brand to safeguard classified information. It is FIPS 140-3 Level 3 (Pending) certified with new enhancements from NIST requiring secure microprocessor upgrades for stronger security and attack protections for government and military uses. Data is encrypted and decrypted on the D500S without any trace left on the host system. Along with hardware-based XTS-AES 256-bit encryption, it features a rugged zinc casing that is waterproof[1], dustproof[1], shock and vibration resistant to military standards[2], crush-resistant and special epoxy-filled to protect internal components from penetration attacks.

IronKey D500S is an essential pillar to meeting Data Loss Protection (DLP) best practices with the toughest military-grade security for compliance with data encryption laws and regulations such as CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX and CCPA, along with TAA. D500S offers more features than any other drive in its class, making it an industry-leading security solution for high-value, confidential data protection.

D500S self-tests upon bootup and over-temperature or voltage conditions will lead to drive shutdown. For added peace of mind, D500S incorporates digitally-signed firmware, making it immune to BadUSB malware. Brute force password attack protection is always on to guard against password guessing and will ultimately crypto-erase the drive if invalid password retries are exceeded.

It offers a Multi-Password option to access data, which supports up to three passwords: Admin, User and One-Time Recovery. Admin can reset a User password and also enable a One-Time Recovery password to restore access if the User password is forgotten.

D500S supports traditional Complex password or Passphrase mode[3]. Passphrases can be from 10–128 characters long. The FBI

recommends multi-word passphrases of 15 or more characters as stronger yet easier to remember than complex passwords.[4]

D500S includes an industry-first Dual Hidden Partition option where Admin can create two custom-sized secure partitions for Admin and User, thereby allowing for a Hidden File Store that can be used to provision files to the User partition as needed. When using untrusted systems or sharing the drive, the Hidden File Stores keep their data secure and invisible unless properly accessed.

With a special key sequence, Admin can enter a Crypto-Erase password that will crypto-erase the drive, destroy the data forever and reset it to prevent unauthorised access in compromising situations.

To assist users with keyboard issues, all password entry screens include an Eye symbol that will display the password entered to reduce typos. A virtual keyboard is also available in English[5] to shield password entry from keyloggers and screenloggers.

D500S also supports two levels of Read-Only (Write-Protect) modes. Both Admin and User can set a session-based Read-Only mode to protect the drive from malware on untrusted systems. Admin can also set a Global Read-Only mode that sets the drive in Read-Only mode until reset.

It also delivers fast dual-channel performance without compromising security. The drive includes a unique 8-digit serial number that is the same electronically as the number engraved on the casing, with a scannable bar code for drive deployment or auditing purposes.

D500S offers many customisation options, is TAA/CMMC compliant and is assembled in the USA.

Managed model

Kingston IronKey D500SM (M = Managed[6]) drives allow central management of drive access and usage across a fleet of drives for larger enterprises or governments.

- FIPS 140-3 Level 3 (Pending) certified for flagship military-grade security
- Multi-Password option with Complex/Passphrase modes
- Industry-first Dual Hidden Partition option
- Crypto-Erase password for compromising situations
- Rugged zinc casing for penetration attack protection, withstands shocks and vibrations to military standards, IP67 waterproof/dustproof[7]
- User-friendly interface
- Fully customisable features
- Available in a Managed model

Key Features

- Military-grade hardware-encrypted USB drive

  FIPS 140-3 Level 3 (Pending) certified XTS-AES 256-bit encryption with secure microprocessor upgrades for stronger security. Built-in protections against BadUSB and brute force attacks. New drive self-tests upon bootup; thermal and voltage protection to automatically shut down drives when they reach certain thresholds.

- Multi-password option for data recovery

  Enable Admin, User and One-Time Recovery passwords. Admin can reset a User password and enable a One-Time Recovery password to restore User's access to data if the User password is forgotten.

- Complex or Passphrase Mode

  Select between Complex or Passphrase mode. Passphrases can be complete sentences or multiple words that only you remember – from 10 to 128 characters long. An eye symbol for all entered passwords helps reduce typos.

- Industry-first Dual Hidden Partition option

  Admin can create two custom-sized Dual Hidden Partitions for Admin and User for a Hidden File Store to keep data secure and invisible unless properly accessed. Dual Hidden Partitions can provide additional security on untrusted systems or when drive sharing is required.

- Crypto-Erase password for compromising situations

  The Crypto-Erase password will wipe encryption keys, delete all data forever and reset the drive.

- Global and Session Read-Only (write protect) modes

  Both Admin and User can set a session-based Read-Only mode to protect the drive from malware on untrusted systems. Admin can also set a Global Read-Only mode that sets the drive in Read-Only mode until reset.

- Rugged casing built to toughest Ironkey standards

  Zinc casing that is crush resistant and epoxy filled for physical tamper-resistant security. MIL-STD-810F-certified for mechanical shock, vibration and drop tests. IP67-certified for waterproof[1] and dustproof[1].

- Unique 8-digit serial number and scannable barcode

  To save time, simply read or scan the barcode when deploying, upon return or during any physical auditing.

- Fully customisable

  Enable, disable, modify drive features and profile. Co-logo.

Specifications

Key certifications	FIPS 140-3 Level 3 (Pending) MIL-STD-810F TAA/CMMC Compliant, Assembled in USA
Interface	USB 3.2 Gen 1
Capacities*	8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB
Connector	Type-A
Speed[8]	USB 3.2 Gen 1 8GB – 128GB: 260MB/s read, 190MB/s write 256GB: 240MB/s read, 170MB/s write 512GB: 310MB/s read, 250MB/s write USB 2.0 8GB – 512GB: 30MB/s read, 20MB/s write
Dimensions	77.9 mm x 21.9 mm x 12.0 mm
Waterproof/Dustproof[9]	IP67 certified
Operating temperature	0℃ to 50℃
Storage temperature	-20℃ to 85℃
Compatibility	USB 3.0/USB 3.1/USB 3.2 Gen 1
Customisation options	D500S: Enable, disable, modify drive features and profile. Co-logo. D500SM: Modify drive profile. Co-logo.

Warranty/support	D500S: 5-year warranty, free technical support D500SM: 2-year warranty, free technical support
Compatible with	Windows® 11, 10, macOS® 11.x – 14.x, Linux[10] Kernel 4.4+

Part Numbers

Serialised drives

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

Serialised Managed Drives

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB
IKD500SM/64GB
IKD500SM/128GB
IKD500SM/256GB
IKD500SM/512GB

Product Image

* Some of the listed capacity on a Flash storage device is used for formatting and other functions and thus is not available for data storage. As such, the actual available capacity for data storage is less than what is listed on the product. For more information go to Kingston's Flash Memory Guide.

1. Please refer to the datasheet specifications. Product must be clean and dry before use.
2. MIL-STD-810F-certified for mechanical shock, vibration and drop tests.
3. Passphrase mode is not supported in Linux.
4. From fbi.gov: Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords, February 18, 2020
5. Virtual keyboard: Only supports US English on Microsoft Windows and macOS.
6. SafeConsole management service purchased separately
7. Product must be clean and dry before use
8. Speed may vary due to host hardware, software and usage.
9. IEC 60529 IPX8-certified as waterproof with the cap on. Product must be clean and dry before use.
10. Feature support on Linux is limited. Refer to user manual for more details. Certain distributions of Linux will require super-user (root) privileges in order to execute the IronKey commands properly in the terminal application window.